Behavioral Analysis on IPv4 Malware on different platforms in IPv6 Network Environment

Zulkiflee M., Azirah S.A., Haniza N., Zakiah A., Shahrin S.
Faculty of Information and Communication Technology
Universiti Teknikal Malaysia Melaka (UTeM), Malacca, Malaysia
zulkiflee@utem.edu.my, azirah@utem.edu.my, haniza@utem.edu.my, zakiah@utem.edu.my,
shahrinsahib@utem.edu.my

***Abstract*- Malware is becoming an epidemic in computer network nowadays. Malware attacks are a significant threat to networks. A conducted survey shows malware attacks may result a huge financial impact. This scenario has become worse when users are migrating to a new environment which is Internet Protocol Version 6. In this paper, a real Nimda worm was released on a network to further understand the worm behavior in real network traffic. A controlled environment of IPv6 networks were deployed as a testbed for this study. The result between these two scenarios on different operating system platforms will be analyzed and discussed further in term of the worm behavior. The experiment result shows that even IPv4 malware still can infect the IPv6 network environment without any modification on the existing malware. In addition, the worm behaves differently in different operating system. A statistical approach will be used to validate the result. New detection techniques need to be proposed to remedy this problem swiftly.**

Keywords: IPv6; malware; IDS

I. INTRODUCTION

IPv6 was introduced as a new network protocols which is meant to overcome IPv4 problems which offering features such as a large number of address flexible addressing scheme, more efficient packet forwarding, more secure communication, better support for mobility and many more [1]. Although IPv6 offers a lot of benefits, people are still reluctant to totally migrate from IPv4 to IPv6 network. This is because even IPv6 have been deployed for many years, this protocol is still considered in its infancy [2]. Many researchers have spent ample of time to enhance the IPv6 services to become at least at par with IPv4 addresses. Since IPv4 addresses are facing depletion, migrating to IPv6 is inevitable eventually [3-5]. Some studies claimed that IPv6 cause many security issues [6-9]. However, researchers pay little attention on IPv6 security issues[10]. In fact, intruders are intended to fully exploit vulnerabilities occur during this transition period. Studies show that new age malwares can survive in new network environment [11, 12]. Hence, researchers agree that further studies have to be conducted to remedy the malware infection issues [13-16].

Malware is software which rapidly invented to manipulate vulnerabilities of computer networks. Based on [17], 250 new malware variants were introduced everyday from all over the world. These so called new age malwares were not totally new genuine ones but rather innovated from the existing malware. These malwares were modified and some modules were added to it to avoid being detected from the anti-virus software which is using signature patterns to detect malwares.

Malware is becoming an epidemic in computer network nowadays[18]. Malware attacks are a significant threat to networks. A conducted survey shows malware attacks may result a huge financial impact[19]. This scenario is becoming worse when users are migrating to a new environment which is IPv6. A study shows that even IPv4 malware still can infect the IPv6 network environment without any modification[20].

Each of different network users has their own needs and preferences[21]. It is a flaw to assume all of network users are using the same operating system even within the same enterprise. Hence, it is necessary to assess the impact of using different operating systems platform in term of malware attack.

The objective of this study is to analyze malware behavior in different operating system platforms namely Windows XP SP1 and Windows Vista SP1.

In the following sections, the paper will explain about some related works to this study and followed by the methodology used in this experimental research. The experimental design will be explained and some result and analysis will be discussed. The Kruskal Wallis Test will be used to validate the difference between data gathered from the testbed simulation. Finally, the conclusion for the overall study will be stated in the end of this paper.

II. RELATED WORK

A. Malware

Malware are represented by several forms namely virus, Trojan, spyware, adware and worms [22, 23]. Each of them has different characteristics to attack their victims. Their method of propagation also varied including sharing memory sticks, downloading files, peer-to-peer applications, sharing file and many more.

Many activities can help these malware propagate more easily. Unfortunately, most of end-users are not fully aware of it due to lack of knowledge about this issue. We have classified this propagation in two categories namely human intervention and self-propagation. In this study, we are focusing on self-propagation category which is worm the only malware form falls in this category [20].

B. The difference between operating systems

Mohamed has conducted studies on the impact of using different operating systems in IPv6 network which a few parameters have been taken into consideration [24, 25]. The study shows different operating systems give impact on its performance due to the difference of its system architecture. Thus, this study is focusing on the difference between two different Windows distributions namely Windows XP and Windows Vista on worm propagation. The study should reveal whether the packet patterns, targeted ports and protocol used are the same between these two operating systems after a node has been infected by a malware.

C. *Worm Propagation Model*

Till this point of time, many researchers had conducted theoretical model studies on worm propagation issues in IPv6 network. The problem with IPv6 network is there is lack of IPv6 data traffic to be used for analysis.

Zhoawen has analyzed the Internet worm modeling in IPv4 and IPv6 [26]. Whereas, Liu has conducted a study on worm behavior in dual-stack network but the result was based on simulation where the seed was based on estimation [27]. While, Zhang has conducted a study and proposed a control mechanism for worm propagation by using SIRS model [28]. In this case, most of the conducted studies have revealed their models which related to the malware propagation. Nevertheless, the models still need to be validated by using a real network environment. As Mehmood said in his paper, the theoretical study is important to understand the basic characteristics about an issue. However, the result must be verified by using a real hardware[29].

Thus, this study is focusing on release a real worm on a real live isolated network to observe its behavior in general. Even so, the result is still can be improved by using more complex network which may replicating a real network environment.

III. METHODOLOGY

In Figure 1, a sequence of schematic work flow has been designed as a process of malware detection.

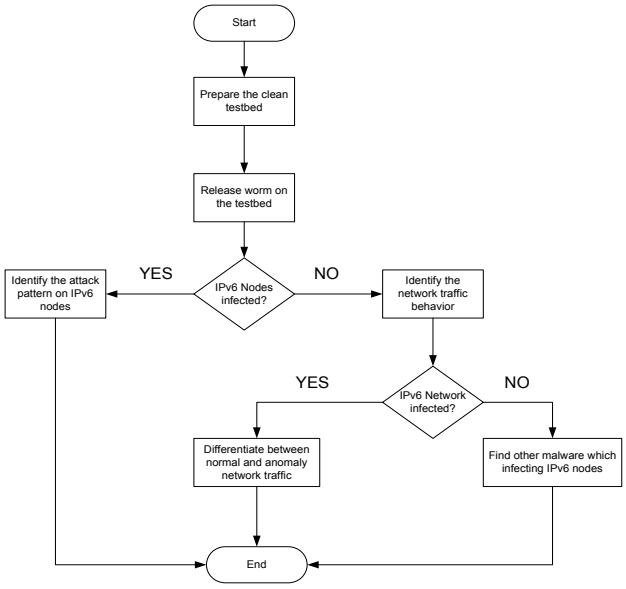

Figure 1: Malware Detection Framework

In order to test the IPv4 worm behavior on different operating system platforms in IPv6 network environment, two testbeds have been implemented. The nodes setup and configuration are identical except for the operating system installed on the computers are different. The testbed designed for this study can be found in Figure 2.

Before the worm released, a clean testbed need to be ready. Some worms will remain in the memory even after the virus was cleaned by the antivirus software. Therefore, each computer was cleaned thoroughly including formatting used computers to ensure no other factors will affect the result later on. The original configuration for computers, router and switch involve were restored.

After the clean testbed ready, the packet sniffer tool was activated to capture all packets through the gateway router. Then, the worm was released at once to allow the worm to propagate the effect throughout the network. The gateway router is essential in this experiment is because to simulate as if this environment is accessible to the other networks. Hence, this design deceived the worm to launch its attack to broader scale rather than local area network only.

A study shows that the IPv4 worm still can survive in IPv6 network environment [20]. Although it not affects IPv6 nodes directly, the attack still cause a lot of bandwidth consumption. A further study needs to be conducted to analyze the impact of the worm attack on different operating system platform in term of bandwidth consumption and port vulnerabilities. Technically, the newer operating system may have sturdier security defense compares to the previous one. Towards the end of this paper, the result will prove whether the common belief is valid or not.

IV. EXPERIMENT DESIGN

In this experiment, the network layout used as depicted in Figure 2. Based on Figure 2, three computers had been setup in this testbed namely PC1, PC2 and PC3. PC1 was installed a packet sniffer software to capture all traffic through the gateway router trunk. PC2 and PC3 work as nodes in the same network where PC2 as the source who release the worm. Each scenario used different operating system platform and Nimda variant E as the worm used in the experiment. Duration for each scenario is about three hours.

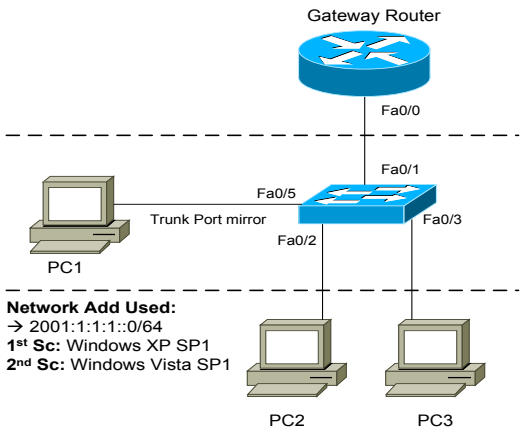

Figure 2: Testbed Network Layout

The procedure of this experiment is as the following:

S1. Ready all computers, router and switch. Restore default configurations into those computers, router and switch.
S2. Leave the computers for two minutes to ensure the network traffic has become stable.
S3. Activate the packet capture software on PC1 to start capture the packet through the gateway link.
S4. Start releases the Nimda.E worm from PC2.
S5. Leave the testbed for three hours to allow some time for the worm to launch its attack on the network.
S6. Plug out all cables connected to computer to stop the simulation and save the network traffic log from PC1 for further analysis.
S7. Before starts the next experiment session, all computers must be formatted to ensure it is free from worm infection in operating system and in its memory.

V. RESULT & ANALYSIS

A. The First Scenario

In this scenario, Windows XP SP1 will be used as the nodes' operating system. The network address used for this scenario is 2001:1:1:1::0/64 as stated in Figure 2. Before we released the worm, we ensure everything properly configured and we left the testbed for a few minutes to make sure the network stabilized.

After the network stable, the packet sniffer in PC1 was activated then the worm released in the network. Each packet through the link between the gateway router and the switch was copied to the trunk port. The packets were captured by a packet sniffer tool which installed in PC1. After three hours duration, the data collection was stopped and the log was saved for further analysis.

Figure 3 shows the sample of packet captured plotted in a line graph. This line represented the total number of packets captured through the gateway router link in bucket of 10 sec. Based on Figure 3, the line was consistently located at 150 units which meant within 10 seconds, 150 packets went through the gateway.

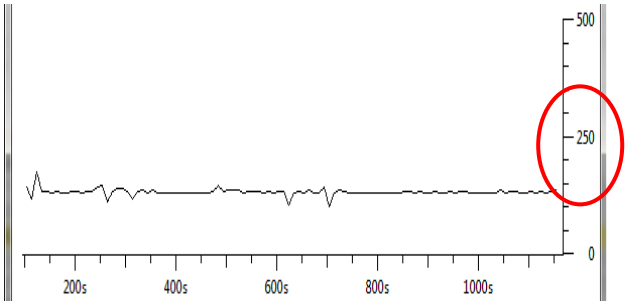

Figure 3: Network Traffic pattern after Nimda.E worm released in Windows XP SP1

Once further analysis on the dataset is completed, the following information was compiled in Table I and Figure 4.

TABLE I: Input from dataset in Scenario 1

Type of Protocol used	UDP, TCP and Others
The Most Type of Protocol used	UDP - 91.35%
Port number connected	67, 137 and 138
The Most Port number connected	67 (Bootstrap Protocol)
Average Number of packet per minute	155.89 pkt/min
Targeted IP Addresses	IPv4 addresses (APIPA)

Based on Table I, some significant information was extracted from the dataset. The most significant protocol used was UDP with more than 91% from the overall packets through the gateway router. The number of vulnerable ports is three and port 67 which was meant for bootstrap protocol scored the highest frequency. In addition, the average number of packets through the gateway router is about 155 packets per minute.

Since the worm used is cultivated only for IPv4 network, hence the targeted IP protocol is IPv4 network. However, there is no valid IPv4 configuration on the node as the node only activated IPv6 network configuration. Hence, the worm launched its attack to Automatic Private IP Addressing (APIPA) which the configuration is automatically configured by Windows operating system if there is no valid network configuration found.

Whereas in Figure 4 shows the distribution of number of packets released by Nimda worm in Windows XP within a minute throughout three hours data collection. From the figure, it can be seen that most of the time, 160 packets went through the gateway router link in a minute. This distribution is normal because it is supported by the fact that the mean and median values are more or less the same which is 159.89 and 160.00 respectively.

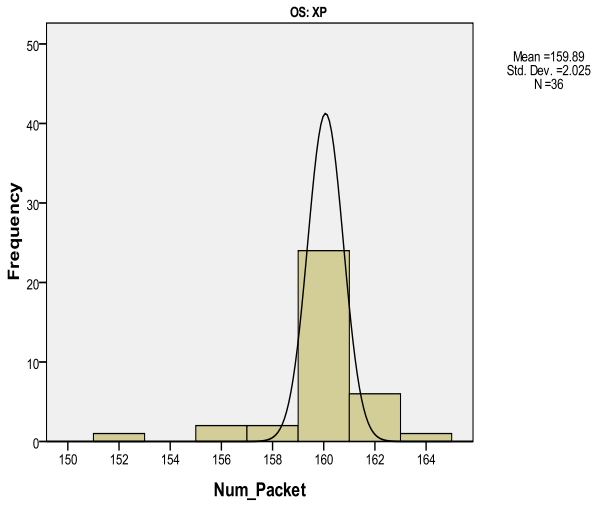

Figure 4: The Distribution of Number of Packet Released by Nimda in Windows XP

B. The Second Scenario

In this scenario the network layout and the computers setup were identical with the previous scenario except Windows Vista SP1 is used as nodes' platform this time. The network address for this scenario is 2001:1:1:1::0/64. The procedure is still the same as in the previous experiment.

Figure 5 shows the sample of packet captured plotted in a line graph. This line represented the total number of packets captured through the gateway router link in bucket of 10 sec. Based on Figure 5, the line was fluctuated around 50 units which meant within 10 seconds, 50 packets went through the gateway.

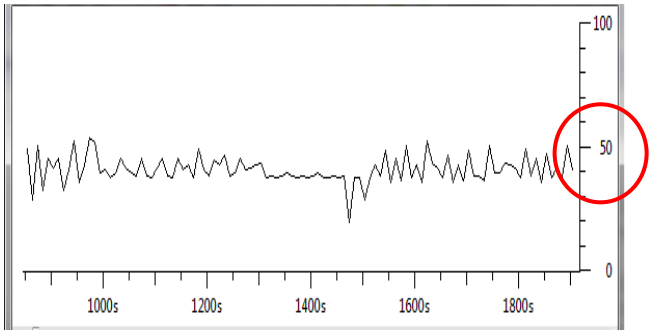

Figure 5: Network Traffic pattern after Nimda.E worm released in Windows Vista SP1

Table II and Figure 6 summarized the result compilation of dataset analysis in Scenario 2.

TABLE II: Input from dataset in Scenario 2

Type of Protocol used	UDP and Others
The Most Type of Protocol used	UDP – 97.7%
Port number connected	67, 137, 138, 3702, 5355 and 1900
The Most Port number connected	1900 (Windows Messenger Broadcast)
Average Number of packet per minute	33.61 pkt/min
Targeted IP Addresses	IPv4 addresses (APIPA)

Based on Table II, some significant information was extracted from the dataset. The most significant protocol used was UDP with more than 97% from the overall packets through the gateway router. The number of vulnerable ports is six and port 1900 which was meant for Windows Messenger Broadcast scored the highest frequency. In addition, the average number of packets went through the gateway router is about 33 packets per minute.

Since this worm used is cultivated only for IPv4 network, hence the targeted IP protocol is IPv4 network. However, there is no valid IPv4 configuration on the node as those nodes only activated IPv6 protocol. Hence, the worm sent packets to APIPA same as in the previous scenario.

Whereas in Figure 6 shows the distribution of number of packets released by Nimda worm in Windows Vista within a minute throughout two hours data collection. From the figure, it shows that the distribution is not normal because it is supported by the fact that mean and median values are different which is 33.61 and 48.00 respectively.

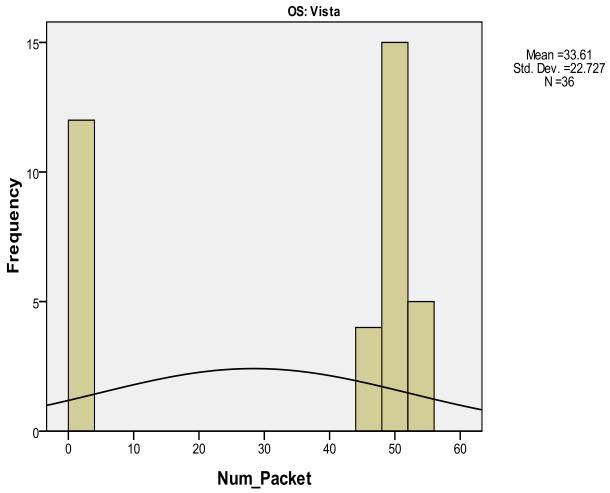

Figure 6: The Distribution of Number of Packets Released by Nimda in Windows Vista

VI. THE EXPERIMENT RESULT ANALYSIS

This paper uses statistical analysis approach to analyses the outputs from both datasets. Based on the distribution patterns of datasets which cannot be assumed as normal distribution, a nonparametric T-test is used to determine for a difference between these two group datasets independently. Kruskal-Wallis is a nonparametric test that able to test whether a single factor can affect a group differently. In this study, kruskal –Walis test is used to determine whether there is difference in number packets sents in a second (Num_Packet) between two observed operating systems. The results of the test are as shown in Table III and Table IV.

Table III is the Rank table shows the both OS are ranked based on the mean rank which XP released more number of packet compares to Windows Vista.

TABLE III: Kruskal Wallis Test

Rank

OS		N	Mean Rank
Num Packet	XP	36	54.50
	Vista	36	18.50
	Total	72	

TABLE IV: Statistical Test Grouping by OS

Test Statistics[a,b]

	Num_Packet
Chi-Square	55.849
df	1
Asymp. Sig.	.000

Meanwhile, Table IV shows the test statistic table to test null hypothesis that the number of packet affected both operating system is same. However, the significant level value *Asymp. Sig.* of P<0.01 in this test statistic

table indicates that there is a significant difference of number packet between Windows XP and Windows Vista.

TABLE V: Comparison between Windows XP and Windows Vista

Item	Windows XP	Windows Vista
The Most Protocol Used	UDP - 91.35%	UDP – 97%
Average Number of Packet Released	155.89 pkt/min	33.61 pkt/min
Number of Vulnerable Port	3	6
The Most Used Port	67 (Bootstrap Protocol)	1900 (Windows Messenger Broadcast)
Targeted IP Protocol	IPv4 Addresses (APIPA)	IPv4 Addresses (APIPA)
Packet Distribution	Normal	Not Normal

Table V shows the comparison the impact of Nimda.E variant impact on Windows XP and Windows Vista platform. Based on the table, it shows that the worm releasing UDP packets when it tries to attack the network. Windows XP shows the worm release a lot more packets compares Windows Vista which mean network with Windows XP will easily congested with packets once this worm attack their network.

The data also shows that Windows Vista has more vulnerable ports shall be taken in consideration compares to Windows XP. The most port used is 1900 which the connections were intended to search for upstream Internet gateway. Further investigation found that all ports which the worm tries to connect have a potential risk for further exploitation.

Since there is no valid IPv4 configuration set on those nodes in the experiment, the worm tended to use Automatic Private IP Addressing (APIPA) as its destination address in both scenarios. APIPA is automatically obtained by a Windows node once it does not have manual IP configuration and it failed to get it from any DHCP server.

In term of packet distribution, Windows XP is easier to identify since it is considered as normal distribution. However, for Windows Vista it is a bit trickier to identify because the packet distribution is not normal as shown in Figure 6.

VII. THE EXPERIMENT FINDINGS

After two different scenarios executed and analyzed the conclusions for this study as the following:

- Even IPv6 node infected, it still look for its victim in IPv4 network. This shows that IPv4 malware still can affect bandwidth consumption in IPv6 network environment without any modification made on the existing worm.
- In term of attack impact, Windows XP is more severe compares to Windows Vista because the number of packets released in Windows XP is really massive which is 155 packets per minute. This mean, Windows Vista has patched some potential risk occurred in Windows XP.
- Windows Vista has more vulnerable ports compares to Windows XP. Even the number of packets was reduced; Windows Vista opens more ports which led to potential risk to its node.
- The malware activity is easier to detect in Windows XP because the packet distribution is normal and can be easily identified by setting normal profile benchmarking. However, it is harder to identify malware attack activities for Windows Vista nodes as the packet distribution is not normal.

VIII. CONCLUSION

Migrating from IPv4 to IPv6 is inevitable. Many researchers put a lot of effort to ensure the IPv6 services and stability to be much better compares to IPv4. However, not many researchers pay enough attention on security issues. The malware give severe impact on the network which cause a lot of trouble to end users. This paper shows that malware which was invented for IPv4 network still can affect IPv6 network without any modification made on the existing malware. Even it does not attack the IPv4 nodes; still it degrades the network performance by releasing a lot of packets which led to bandwidth consumption. The use of different operating system gives different impact on the network. A new operating system is not a total solution to solve problems occurred in the previous version operating system. Without proper monitoring and management, the impact cannot be expected even when we are using a newer operating system. The operating system is always needed to be patched from time to time to ensure the node will become safer from any type of attacks.

For further research, a more realistic testbed need to be used to represent the real network environment. A heterogeneous platforms need to used as its give different impact on the malware propagation. Furthermore, a study on how this worm behaves in transition mechanism such as dual-stack also needs to be conducted to further understand how the malware works. Finally, a new detection technique needs to be proposed to cater this issue.

ACKNOWLEDGEMENT

The research presented in this paper is supported by University of Technical Malaysia Malacca (UTeM) under a short-term grant project (PJP/2011/FTMK(14A)/ S00896) which was conducted at Faculty of ICT (FTMK).

REFERENCES

[1] Waddington, D.G. and F. Chang, *Realizing the transition to IPv6.* IEEE Communications Magazine, 2002. **40**(6): p. 138-147.

[2] Ismail, M.N. and Z.Z. Abidin. *Implementing of IPv6 Protocol Environment at University of Kuala Lumpur: Measurement of IPv6 and IPv4 Performance*. in *Future Computer and Communication, 2009. ICFCC 2009. International Conference on*. 2009.

[3] Zheng, Q., T. Liu, X. Guan, Y. Qu, and N. Wang, *A new worm exploiting IPv4-IPv6 dual-stack networks*, in *Proceedings of the 2007 ACM workshop on Recur-*

ring malcode. 2007, ACM: Alexandria, Virginia, USA.

[4] Hua, N. *IPv6 test-bed networks and R&D in China*. in *Applications and the Internet Workshops, 2004. SAINT 2004 Workshops. 2004 International Symposium on*. 2004.

[5] Kamra, A., H. Feng, V. Misra, and A.D. Keromytis. *The effect of DNS delays on worm propagation in an IPv6 Internet*. in *INFOCOM 2005. 24th Annual Joint Conference of the IEEE Computer and Communications Societies. Proceedings IEEE*. 2005.

[6] Badamchizadeh, M.A. and A.A. Chianeh. *Security in IPv6*. in *Proceedings of the 5th WSEAS International Conference on Signal Processing*. 2006. Istanbul, Turkey.

[7] Warfield, M.H., *Security Implications of IPv6.* Retrieved April, 2003. **30**: p. 2006.

[8] Sharma, V., *IPv6 and IPv4 Security challenge Analysis and Best-Practice Scenario.* International Journal of Advanced of Networking and Applications, 2010. **01**(04): p. 258-269.

[9] Yuce, E., *A CASE STUDY ON THE SECURITY OF IPV6 TRANSITION METHODS.* ACM Workshop on Recurring Malcode, 2009.

[10] Zhao-wen, L.I.N., W. Lu-hua, and M.A. Yan, *Possible Attacks based on IPv6 Features and Its Detection.* Network Research Workshop, APAN, 2007.

[11] Gold, S., *The changing face of malware.* Computer Fraud & Security, 2009. **2009**(9): p. 12-14.

[12] de la Cuadra, F., *The geneology of malware.* Network Security, 2007. **2007**(4): p. 17-20.

[13] Hansman, S. and R. Hunt, *A taxonomy of network and computer attacks.* Computers & Security, 2005. **24**(1): p. 31-43.

[14] Bellovin, S.M., B. Cheswick, and A.D. Keromytis, *Worm propagation strategies in an IPv6 Internet.* LOGIN: The USENIX Magazine, 2006. **31**(1): p. 70-76.

[15] Zagar, D., K. Grgic, and S. Rimac-Drlje, *Security aspects in IPv6 networks-implementation and testing.* Computers & Electrical Engineering, 2007. **33**(5-6): p. 425-437.

[16] Jordan, C., A. Chang, and K. Luo. *Network Malware Capture*. 2009: IEEE Computer Society.

[17] Stewart, J., *Behavioural malware analysis using sandnets.* Computer Fraud & Security, 2006. **2006**(12): p. 4-6.

[18] Lelarge, M. *Economics of malware: Epidemic risks model, network externalities and incentives*. in *Communication, Control, and Computing, 2009. Allerton 2009. 47th Annual Allerton Conference on*. 2009.

[19] Computer Economics, *Annual Worldwide Economic Damages from Malware Exceed $13 Billion*. 2007.

[20] Zulkiflee, M., M.A. Faizal, I.O. Mohd Fairuz, A. Nur Azman, and S. Shahrin, *Behavioral Analysis on IPv4 Malware in both IPv4 and IPv6 Network Environment.* International Journal of Computer Science and Information Security (IJCSIS), 2011. **9**(2).

[21] Li, Q., J. Zhou, Q.-R. Peng, C.-Q. Li, C. Wang, J. Wu, and B.-E. Shao, *Business processes oriented heterogeneous systems integration platform for networked enterprises.* Computers in Industry, 2010. **61**(2): p. 127-144.

[22] Karresand, M., *A proposed taxonomy of software weapons.* No. FOI, 2002.

[23] Robiah, Y., S.S. Rahayu, M.M. Zaki, S. Shahrin, M.A. Faizal, and R. Marliza, *A New Generic Taxonomy on Hybrid Malware Detection Technique.* Arxiv preprint arXiv:0909.4860, 2009.

[24] Mohamed, S.S., A.Y.M. Abusin, and D. Chieng. *Evaluation of IPv6 and comparative study with different operating systems*. in *Information Technology and Applications, 2005. ICITA 2005. Third International Conference on*. 2005.

[25] Mohamed, S.S., M.S. Buhari, and H. Saleem, *Performance comparison of packet transmission over IPv6 network on different platforms.* Communications, IEE Proceedings-, 2006. **153**(3): p. 425-433.

[26] Zhaowen, L., S. Fei, and M. Yan. *The analysis of Internet worm modeling in IPv4 and IPv6 networks*. in *Broadband Network and Multimedia Technology (IC-BNMT), 2010 3rd IEEE International Conference on*. 2010.

[27] Liu, T., X. Guan, Q. Zheng, and Y. Qu, *A New Worm Exploiting IPv6 and IPv4-IPv6 Dual-Stack Networks: Experiment, Modeling, Simulation and Defense*. 2009, IEEE Network.

[28] Zhang, D. and W. Ye. *SIRS: Internet Worm Propagation Model and Application*. in *Electrical and Control Engineering (ICECE), 2010 International Conference on*. 2010.

[29] Mehmood, A., O. Hohlfeld, D. Levin, A. Wundsam, F. Ciucu, F. Schneider, A. Feldmann, and R.-P. Braun, *The Routerlab - Emulating Internet Characteristics in a Room.* Photonic Networks, 2010 ITG Symposium on, 2010: p. 1-8.